X.509 Copenhagen editing meeting Oct 27-29, 1999

Overview of major changes

Sharon Boeyen

Entrust Technologies

X.509 (2000): Status

- FPDAM editing meeting held Oct 27-29
- Editing task currently underway, including DCOR
  - Available on bull site once approved by participants
- Deadline for text to ISO and ITU: Nov 20
  - No further changes (except editorial and bug fixes)
- Revised draft expected to progress to DAM stage
- Expected next steps:
  - Approval by ITU for 6 week ***Y/N*** ballot - March 2000
  - ISO ***Y/N*** DAM ballot to follow ITU approval
  - International Standard before year end 2000

PKIX raised issues: update

- Interpretation of basicConstraints absence in v3 cert
  - No fix will be made to 97 text
  - 2000 text will state that absence means end-entity cert

- Version of CRL that contains no critical extensions
  - 97 text will be fixed and 2000 text will align with fix
    - A CRL that does not contain any critical extensions may be marked as either a v1 or a v2 CRL

PKI Extensions added since 97

- Certificate extensions added
  - inhibitAnyPolicy*
  - freshestCRL
  - *(nameMapping was added in Apr, but deleted at this meeting)**
  - CRL extensions
  - crlScope
  - orderedList
  - crlStreamIdentifier
  - statusReferral
  - deltaInfo (in FPDAM was bundled with crlScope)*
  - baseUpdateTime (for use in delta CRLs)

(* denotes Copenhagen change)

PKI Schema added since 97 text

Object classes

- pkiUser
- pkiCA
- deltaCRL
- cpCps
- pkiCertPath*

Attributes

- certificationPracticeStmt
- certificatePolicy
- pkiPath*

(* denotes Copenhagen change)

(relevant matching rules also added for attributes and for extensions)

PKI Defect Reports

- Current DCOR ballots close Nov 5
  - No major problems anticipated
  - DCOR 7 (policy processing) has comments at least from US and Canada for clarification of proposed text
  - expect fixes to be approved for 97 text and folded into 2000 text as well
- New defect report on Authority Key Identifier
  - Not yet processed

PKI Clarifications

- New text around ‘overlapping’ CRLs was confusing and is being clarified
- Many changes in the definitions section (mainly shortening them)
- New terms and acronyms added for specific CRL types to enable clearer writing, especially with addition of attribute certificate revocation list types (e.g. EPRL, EARL, AARL, CARL)
- Complete restructuring of 509 into 4 sections moving Directory usage related material to end

PMI: major editorial changes

- Major clarification of models section
- Restructuring of extensions section by functional areas (similar to PKI extensions section)
- Terminology changes
  - owner > holder
  - claimant > privilege asserter
  - verifier > privilege verifier
- Optional delegation & roles functions clarified
- Updates to definitions

PMI: major technical changes

- Indirect delegation of privilege deleted
  - indirectIssuer and delegatorAttributeId extensions deleted
- Cross-domain certificate chains deleted
  - crossPrivilege extension deleted
- Attribute certificate syntax extended
  - Object digest info enhanced to enable hash of public key or public key certificate as well as other objects
  - Object digest info added as optional component to issuer
- Linkage between role cert (if there is one) and cert that assigns individual to role described

Major changes to PMI extensions

- Extensions added
  - targetingInformation
  - noRevAvail
- Extensions simplified
  - sOAIdentifier
  - attributeDescriptor
  - ownerAttributeIdentifier > roleCertSpecIdentifier
  - attributeNameConstraints > delegatedNameConstraints
  - authorityAttributeIdentifier
- Specified valid cert types (attribute or public-key or both) and valid holders (I.e. SOA, AA, end-entity)
- Extensions deleted (see previous slide)

Complete list of PMI extensions

General

- timeSpecification
- targetingInformation*
- userNotice

Revocation related

- crlDistributionPoints
- noRevAvail*

SOA related

- sOAIdentifier
- attributeDescriptor

Role related

- roleSpecCertIdentifier

Delegation related

- basicAttConstraints
- delegatedNameConstraints
- acceptableCertPolicies
- authorityAttributeIdentifier

Path processing procedure

- Basic procedure added
  - Relevant to all paths
  - Linkage with PKI certification path processing clarified
- Roles procedure separated into sub-clause
- Delegation procedure
  - Separated into sub-clause
  - Simplified to reflect deletion of indirect delegation and cross privileges
  - Clarified as only required by privilege verifiers in environments where delegation is done

PMI schema: complete list of object classes

- pmiUser
- pmiAA
- pmiSOA
- attCertCRLDistributionPt
- pmiDelegationPath*
- privilegePolicy*

(* denotes new object classes added at Copenhagen)

PMI: complete list of attributes

- attributeCertificateAttribute
- aaCertificate
- attributeDescriptorCertificate
- attributeCertificateRevocationList
- attributeAuthorityRevocationList
- delegationPath*
- privPolicy*

(* denotes new object classes added at Copenhagen)

(relevant matching rules also added for attributes and for extensions)